IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of: Julian DURAND et al.		Atty. Docket No.:	004770.00581
Serial No.:	09/893,589	Group Art Unit:	2143
Filed:	June 29, 2001	Examiner:	Truong, Lan Dai T
For:	SYSTEM FOR PROTECTING COPYRIGHTED MATERIALS	Confirmation No.:	5623

APPEAL BRIEF

U.S. Patent and Trademark Office
Customer Service Window, Mail Stop Appeal Brief - Patents
Randolph Building
401 Dulany Street
Alexandria, VA 22314

Sir:

In response to the Notification of Non-Compliant Appeal Brief mailed June 5, 2006, this is a Replacement Appeal Brief in accordance with 37 C.F.R. § 41.37 in support of Appellants' January 31, 2006, Notice of Appeal. Appeal is taken from the Final Office Action mailed August 25, 2005 (hereinafter, Office Action), and the Advisory Action mailed December 15, 2005 (hereinafter, Advisory Action). Please charge any necessary fees in connection with this Appeal Brief to our Deposit Account No. 19-0733.

REAL PARTY IN INTEREST

37 C.F.R. § 41.37(c)(1)(i)

The owner of this application, and the real party in interest, is NOKIA, Corporation

RELATED APPEALS AND INTERFERENCES

37 C.F.R. § 41.37(c)(1)(ii)

There are no related appeals and interferences.

STATUS OF CLAIMS

37 C.F.R. § 41.37(c)(1)(iii)

Claims 1-7, 9, 11-16, and 19-22 are rejected. Claims 8, 10, and 17-18 are canceled. Only pending claims 1-7, 9, 11-16, and 19-22 are shown in the attached appendix.

Appellants hereby appeal the rejection of claims 1-7, 9, 11-16, and 19-22.

STATUS OF AMENDMENTS

37 C.F.R. § 41.37(c)(1)(iv)

The Amendment and Response filed November 29, 2005, which is responsive to the Office Action, has not been entered. However, all prior amendments have been entered.

SUMMARY OF CLAIMED SUBJECT MATTER

37 C.F.R. § 41.37(c)(1)(v)

In making reference herein to various portions of the specification and drawings in order to explain the claimed invention, Appellants do not intend to limit the claims; all references to the specification and drawings are illustrative unless otherwise explicitly stated.

The present invention is directed to methods and systems for protecting copyrighted materials. *Original Specification*, p. 1, ll. 4-6; *Substitute Specification*, p. 1, ll. 4-6. According to one embodiment, a system 10 for protecting copyrighted materials includes a central server 12 which includes a trusted lock. The trusted lock ensures to the copyright owners or to parties which want to restrict access to stored content that the server 12 and associated devices with it may be accessed by only devices that are authorized to do so after they have been authenticated. Copyrighted content may be stored in a storage device 16. The copyrighted content may be stored in a protected form, such as encryption. A digital rights management engine 18 is connected to the server 12 to determine appropriate access rights connected to each part of the data content and whether a requesting party has appropriate rights. An audit trail storage device

20 maintains records. *Original Specification*, p. 4, ll. 10-18; *Substitute Specification*, p. 4, l. 24 to p. 5, l. 10; and Figure 1.

In an illustrative operation, a user uses wireless device 14 to contact server 12 where an authentication method is performed using known mechanisms such as Diffie-Hellmann Exchange of Secrets. *Original Specification*, p. 4, ll. 19-21; *Substitute Specification*, p. 5, ll. 11-13. Server 12 receives a request for data from the device 14 and records situation information, such as the time of the request and passes the request onto a digital rights management engine 18. *Original Specification*, p. 4, ll. 24-25; *Substitute Specification*, p. 5, ll. 16-18. If the user has sufficient rights, authorization is provided to the server 12 where the authorization is stored in an audit trail storage device 20. *Original Specification*, p. 4, l. 25 to p. 5, l. 3; *Substitute Specification*, p. 5, ll. 20-22. Server 12, digital rights management engine 18, content storage device 16, and audit trail storage device 20 are shown separate from user device 14 as user device 14 communicates wirelessly with server 12. *Original Specification*, p. 4, ll. 13-18; *Substitute Specification*, p. 5, ll. 2-10, and Figure 1. Step 108 of Figure 3 illustrates an example of how content may be rendered by server 12. *Original Specification*, p. 5, ll. 18-19; *Substitute Specification*, p. 6, ll. 17-18; and Figure 3.

In another embodiment, a user uses a wireless device 14 to contact a server 12. *Original Specification*, p. 4, l. 19; *Substitute Specification*, p. 5, l. 11. An authentication method is performed using known mechanisms. *Original Specification*, p. 4, ll. 19-21, p. 5, ll. 14-15; *Substitute Specification*, p. 5, ll. 11-13, p. 6, ll. 12-14; and Figure 3, step 100. Once both parties are sure of the identity of the other, the user of the wireless device 14 may request data 16 to be sent. *Original Specification*, p. 4, ll. 21-22, p. 5, ll. 15-16; *Substitute Specification*, p. 5, ll. 13-

14, p. 6, l. 14; and Figure 3, step 102. Server 12 receives the request, records situation information of the request, and passes the request to a digital rights management engine 18. *Original Specification*, p. 4, ll. 24-25, p. 5, ll. 15-17; *Substitute Specification*, p. 5, ll. 16-18, p. 6, ll. 14-15; and Figure 3, step 102. Digital rights management engine 18 compares the request with its stored knowledge of the requesting user's right to access the copyrighted or accessed restricted materials. If the user of the wireless device has sufficient rights, authorization is provided to the server 12. *Original Specification*, p. 4, l. 25 to p. 5, l. 2, p. 5, ll. 17-18; *Substitute Specification*, p. 5, ll. 18-21, p. 6, ll. 15-16; and Figure 3, step 104. When the server 12 receives the authorization, it is recorded in an audit trail storage device 20. *Original Specification*, p. 5, ll. 2-3 and 18; *Substitute Specification*, p. 5, ll. 21-24, p. 6, ll. 16-17; and Figure 3, step 106. The data 16 is then formatted and sent by the server 12 to the wireless device 14. *Original Specification*, p. 5, l. 5 and ll. 18-19; *Substitute Specification*, p. 5, l. 25 to p. 6, l. 1, p. 17-18; and Figure 3, step 108.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

37 C.F.R. § 41.37(c)(1)(vi)

Claims 1-3, 6-7, 11-15, and 19-22 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Marconcini *et al.* (U.S. Pat. No. 6,834,110, hereinafter *Marconcini*) in view of Dimenstein (U.S. Pat. No. 6,917,923, hereinafter *Dimenstein*).

Claims 4-5, 9, and 16 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over *Marconcini* in view of *Dimenstein* and further in view of Laursen *et al.* (U.S. Pat. No. 6,065,120, hereinafter *Laursen*).

ARGUMENT

37 C.F.R. § 41.37(c)(1)(vii)

Claims 1-3, 6-7, 11-15, and 19-22 are patentable over *Marconcini*, in view of *Dimenstein*.

The Office Action rejects claims 1-3, 6-7, 11-15, and 19-22 as being unpatentable over *Marconcini* in view of *Dimenstein*. Appellants respectfully traverse this rejection for the reasons stated below. Appellants respectfully traverse the rejection. Appellants note that claim 22 does not appear to be explicitly rejected. However, the Office Action alleges the rejection of claim 1 is "exemplary" of claim 22. (Office Action, page 2).

In order establish a prima facie case of obviousness under 35 U.S.C. § 103(a), three criteria must exist: 1) there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine the reference teachings; 2) there must be a reasonable expectation of success; and 3) the prior art reference(s) must teach or suggest all the claim limitations. *See* MPEP § 706.02 (j); *In re Vaeck*, 947 F.2d 488 (Fed. Cir. 1991).

Regarding the first of the three criteria, the Office Action and the Advisory Action do not establish a prima facie case of obviousness because there is no motivation or suggestion to combine the two references. The Federal Circuit has repeatedly stated that the limitations of a claim in a pending application cannot be used as a blueprint to piece together prior art in hindsight, *In re Dembiczak*, 50 U.S.P.Q.2d 1614 (Fed. Cir. 1999), and that the Patent Office should *rigorously* apply the requirement that a teaching or motivation to combine prior art references needs to be provided. *Id.* (emphasis added). Appellants maintain that there is no motivation or suggestion to combine *Marconcini* with *Dimenstein*.

Marconcini describes a method for securely providing data to a user's system over a broadcast infrastructure. (*Marconcini*, Abstract). In *Marconcini*, a Secure Container (SC), with content and an encryption key, is sent directly from a Secure Container Packet Tool 151 within a Clearinghouse to an End-User Device 109. (*Marconcini*, Figs. 1A-1D and col. 13, l. 47 – col. 14, l. 51). *Dimenstein*, on the other hand, describes a method for ensuring that a digital storage device will only be able to download or play files that were obtained from sources deemed, either by a manufacturer of a device or by an overseeing organization, to be acceptable. (*Dimenstein*, Abstract). The architecture of *Dimenstein* provides a framework for approval of web sites configured to

provide content to users. (*Dimenstein*, Abstract, Summary, Detailed Description, and Claims). *Dimenstein* does not teach or suggest that its web site approval system should be configured to take into account user rights associated with requested data. In addition, *Marconcini* does not suggest that it's Secure Containers with content and encryption keys should be transmitted through a server including a trusted lock. One of ordinary skill in the art at the time of the present invention would not have thought to combine such systems.

As motivation to combine *Marconcini* with *Dimenstein*, the Office Action states, "it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Dimenstein's ideas of submit[ting] their websites to an industry committee. After authorization, the file is downloaded and then encoded with Marconcini's system in order to protect copyright, see (Dimenstein: Column 1, line 64)." (Office Action, page 5). Again, this is not a motivation to combine references. The Clearinghouse of the *Marconcini* system clears only authorized and appropriate usage requests and will not clear bogus requests from unknown or unauthorized parties. (Col. 10, ll. 27-30). Differently, the "industry committee" of *Dimenstein* approves web sites that a user may access. (Col. 3, ll. 24-26, emphasis added). *Marconcini* processes requests for access to content based upon some attribute of an end device (i.e., whether authorized). Under *Marconcini*, an intermediary server is irrelevant. *Dimenstein*, on the other hand, processes requests for access to content based upon an attribute of a web site. So, under *Dimenstein*, an end user is irrelevant. As such, Appellants respectfully submit that that there is no motivation or suggestion to combine *Marconcini* with *Dimenstein*.

Still further, even assuming, without admitting, that the combination of *Marconcini* and *Dimenstein* is proper, Appellants maintain that the combination fails to teach or suggest each and every feature of Appellants' claim 1. In rejecting claim 1, the Office Action alleges that *Marconcini* teaches many of the features of the claim, but admits that *Marconcini* fails to teach, "wherein said data is rendered by said server." (Office Action, page 5). To cure the deficiencies of *Marconcini*, the Office Action relies on *Dimenstein*.

Specifically, the Office Action states, "[h]owever Dimenstein discloses 'the maintainer of websites' which is equivalent to 'a server' submit their website to 'an industry committee' which is equivalent to 'rights management engine'. After going through authentication steps, the file is downloaded in unencrypted format and then encoded: column 7, lines 55-64; column 2, lines 30-34;

column 3, lines 21-44." (Office Action, page 5). Under the *Dimenstein* system, an IP address of a web site is checked against a database of web sites approved by an industry committee. Under the *Dimenstein* system, the industry committee **approves web sites associated with data, not user rights**. Appellants' claim 1 recites, "a rights management engine in communication with said server for applying and enforcing user rights associated with said data." (Emphasis added). Under the *Dimenstein* system, a web site that a user may access is approved for providing content; user rights are never applied or enforced.

As the combination of *Marconcini* and *Dimenstein* fails to teach or suggest each and every feature and is an improper combination based upon a lack of motivation, Appellants respectfully request withdrawal of the present rejection. Appellants' claims 2-3 and 21-22, which depend from claim 1, are allowable over the combination of *Marconcini* and *Dimenstein* for at least the same reasons as their ultimate base claim and further in view of the novel features recited therein.

Appellants' independent claims 6, 13, and 19 include many of the same or similar features as recited above with respect to claim 1. For similar reason as provided above, the motivation to combine *Marconcini* and *Dimenstein* is improper for claims 6, 13, and 19, and Appellants' claims 6, 13, and 19 are patentably distinct over the art of record. Withdrawal of the rejection is respectfully requested. Claims 7, 11-12, 14-15, and 20, which depend from claims 6, 13, and 19, are allowable for all the reasons given above concerning their respective base claims, and further in view of the novel features recited therein

Claims 4-5, 9, and 16 are patentable over *Marconcini*, in view of *Dimenstein*, and further in view of *Laursen*.

The Office Action rejects claims 4-5, 9, and 16 as being unpatentable over *Marconcini* in view of *Dimenstein*, and further in view of *Laursen*. Appellants respectfully traverse this rejection for the reasons stated below.

As stated above, the combination of *Marconcini* and *Dimenstein* is improper and fails to teach or suggest each and every feature of Appellants' claims 1, 6, 13, and 19. The addition of *Laursen*, even if proper, fails to cure these deficiencies. Therefore, claims 4-5, 9, and 16, which

depend from claims 1, 6, and 13, are allowable for at least the same reasons given above concerning their respective base claims, and further in view of the novel features recited therein.

CONCLUSION

For all of the foregoing reasons, Appellants respectfully submit that the final rejection of claims 1-7, 9, 11-16, and 19-22, is improper and should be reversed.

Respectfully submitted,

BANNER & WITCOFF, LTD.

Dated: June 30, 2006

By: /John M. Fleming/
John M. Fleming
Registration No. 56,536

1001 G Street, N.W.
Washington, D.C. 20001-4597
Tel: (202) 824-3000
Fax: (202) 824-3001

BCW/JMF

CLAIMS APPENDIX

37 C.F.R. § 41.37(c)(1)(viii)

1. A system for communicating data and protecting rights therein, comprising:

at least one user device which communicates wirelessly and is capable of performing a mutual authentication with a server for receiving data;

a server in communication with said at least one user device and including a trusted lock;

a rights management engine in communication with said server for applying and enforcing user rights associated with said data;

a storage device in communication with said server for storing said data; and

a storage device in communication with said server for recording a time stamped and digitally signed audit trail;

wherein said server, said rights management engine, said storage device for storing said data and said storage device for recording a time stamped and digitally signed audit trail are separate from said at least one user device, and wherein said data is rendered by said server.

2. The system according to claim 1, wherein said server, rights management engine, data storage and audit trail storage are in a secure location separate from the user device so that trusted services including timing, auditing and copying are performed in a secure environment.

3. The system according to claim 1, wherein said user device includes a storage device for holding data which is released under instructions from said server.

4. The system according to claim 1, wherein said user device is a wireless communication terminal selected from the group consisting of a mobile station, a WAP-capable cellular telephone, an extended markup language capable cellular telephone, or a cellular telephone with a processor-based system connected to it.

5. The system according to claim 4, wherein said wireless terminal is an "always on" device.

6. A method of communicating data from a server to a wireless user device and protecting rights therein, comprising:

authenticating identification of said server and said user device;

requesting data to be communicated from said server to said user device;

authorizing said data to be communicated based on rights attributed to said user device in a rights management engine separate from said user device;

recording said authorization to provide for billing information and an audit trail separate from said user device;

rendering said data from said server to said user device wirelessly.

7. The method according to claim 6, wherein said data is communicated to said user device and stored therein and rendered in sections according to instructions communicated from said server.

9. The method according to claim 6, wherein said wireless user device is an "always on" user device.

11. The method according to claim 6, wherein said recording step is performed in a storage device to record authorization along with time and other information in order to provide a trusted audit trail, which is based on trusted time and a trusted third party to sign the recording.

12. The method according to claim 6, wherein said data is originally stored in a content storage device connected to said server.

13. A rights secure communication device for wirelessly providing data to a user device comprising:

a server, which is capable of performing a mutual authentication with the user device and rendering said data to said user device;

a data storage device connected to said server for storing said data; and

a digital rights management engine connected to said server for determining rights attributed to authenticated users.

14. The communication device according to claim 13, further comprising a secure storage device for recording authorization of data communication in a secure audit trail.

15. The communication device according to claim 13, wherein data is sent from said server to a user through a wireless communication system.

16. The communication device according to claim 15, wherein said wireless communication system is an "always on" connection.

19. A computer program embodied on a computer readable medium and executable by a computer to communicate data having protected rights, the program, when executed, performing the steps of comprising:

communicating wirelessly with a mobile terminal controlled by a user;

determining rights of said user in protected data using a rights management engine;

recording an audit trail of communications with said mobile terminal in a storage device; and

rendering said data and wirelessly communicating said data to said mobile terminal.

20. A computer program according to claim 19, when executed further performing the step of storing said protected data in a secure location separate from said mobile terminal wherein all operations regarding said protected data are performed in a secure environment.

21. The system according to claim 1, wherein said data is stored in protected form.

22. The system according to claim 1, wherein said data rendered by the server is formatted and delivered to said at least one user device for use.

EVIDENCE APPENDIX

37 C.F.R. § 41.37(c)(1)(ix)

None.

RELATED PROCEEDINGS APPENDIX

37 C.F.R. § 41.37(c)(1)(x)

None.